REMARKS

In view of the following discussion, the Applicants submit that none of the claims now pending in the application is anticipated under the provisions of 35 U.S.C. § 102 or made obvious under the provisions of 35 U.S.C. § 103. Thus, the Applicants believe that all of these claims are now in allowable form.

In addition, the Applicants' representative would like to thank Examiner Patel for kindly taking a substantial amount of time on February 14, 2006 to discuss the merits of the subject invention. The Applicants' representative is aware of the time constraint that is placed on the Examiner and is appreciative of the Examiner's willingness to devote such large quantity of time to discuss the case on the merits.

I. REJECTION OF CLAIMS 1-3, 18-20 AND 35-37 UNDER 35 U.S.C. § 102

Claims 1-3, 18-20 and 35-37 stand rejected as being anticipated by the Bots et al. patent (United States Patent No. 6,226,748, issued May 1, 2001, hereinafter "Bots"). In response, the Applicants have amended independent claims 1, 18 and 35, from which claims 2-3, 19-20 and 36-37 depend, in order to more clearly recite aspects of the present invention.

Particularly, the Examiner's attention is directed to the fact that Bots fails to disclose or suggest the novel invention of a virtual private network (VPN) in which master nodes control admission and departure in the VPN for an associated non-empty subset of member nodes, as well as facilitate VPN communications between the member nodes, as claimed in Applicants' amended independent claims 1, 18 and 35.

In contrast, Bots at most teaches a security device (*i.e.*, a VPN unit or VPNU) that intercepts communications en-route between member nodes of VPNs. For example, a VPNU may reside between a local area network's (LAN) router and a public network. The VPNU acts as a site protector for the LAN by intercepting communications leaving and entering the LAN. If both the sender and receiver of the communication are members of a common VPN group, the VPNU must process the communication (*e.g.*, encrypt or decrypt) before allowing the communication to proceed to the intended recipient (*i.e.*, in accordance with handling guidelines for the implicated

PAGE 17/22 * RCVD AT 2/16/2006 6:10:36 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/32 * DNIS:2738300 * CSID:732 530 9808 * DURATION (mm-ss):07-42

VPN group). On the other hand, if the sender and the receiver are not both members of a common VPN group, the VPNU either does nothing to the communication or discards the communication. Thus, a VPNU is not the same as a master node that facilitates communications between member nodes of a VPN, as claimed by the Applicants. The master nodes of the Applicants' invention thereby distribute management responsibilities (*e.g.*, encryption key distribution) in the VPN, making the VPN more easily scalable. In this manner, a master node as claimed by the Applicants may be considered analogous to a conference bridge, where multiple "conference bridges" are implemented to "patch" subsets of users into a common "conference".

Notably, Applicants' invention positively claims master nodes that control admission and departure in a VPN for an associated non-empty subset of member nodes, as well as facilitate VPN communications between the member nodes, as claimed in Applicants' independent claims 1, 18 and 35. Specifically, Applicants' claims 1, 18 and 35, as amended, positively recite:

1. A group management system comprising:
a plurality of interconnected nodes communicatively coupled with each other as member nodes of a virtual private network ("VPN"), wherein all communications between said interconnected nodes are encrypted; and
a plurality of master nodes, each of the master nodes controlling admission and departure in the VPN for an associated non-empty subset of the member nodes and further facilitating said communications between said plurality of interconnected nodes, wherein in the event one of the master nodes fails, the associated subset of member nodes will be automatically reassigned to one or more other of the master nodes. (Emphasis added)

18. A method for managing a group, the method comprising:
providing a plurality of interconnected nodes communicatively coupled with each other as member nodes of a virtual private network ("VPN"), wherein all communications between said interconnected nodes are encrypted; and
providing a plurality of master nodes, each of the master nodes controlling admission and departure in the VPN for an associated non-empty subset of the member nodes and further facilitating said communications between said plurality of interconnected nodes, wherein in the event one of the master nodes fails, the associated subset of member nodes will be automatically reassigned to one or more other of the master nodes. (Emphasis added)

PAGE 18/22 * RCVD AT 2/16/2006 6:10:36 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/32 * DNIS:2738300 * CSID:732 530 9808 * DURATION (mm-ss):07-42

35. A computer readable medium containing an executable program for managing a group, where the program performs the steps of:

providing a plurality of interconnected nodes communicatively coupled with each other as member nodes of a virtual private network ("VPN"), wherein all communications between said interconnected nodes are encrypted; and

providing a plurality of master nodes, each of the master nodes controlling admission and departure in the VPN for an associated non-empty subset of the member nodes and further facilitating said communications between said plurality of interconnected nodes, wherein in the event one of the master nodes fails, the associated subset of member nodes will be automatically reassigned to one or more other of the master nodes. (Emphasis added)

The Applicants' invention is directed to systems and methods for scalable distributed management of virtual private networks (VPNs). The management of encrypted group communications necessary to establish secure, private VPN communications channels through an underlying public network infrastructure places a variety of burdens on a VPN manager. In particular, the addition or removal of a member from a VPN often involves the generation and distribution of one or more new encryption keys that allow current VPN members to decrypt private communications sent through the VPN, but prevent non-VPN members from decrypting the communications. As VPN membership increases and changes dynamically with greater frequency, the complexity of encryption key management becomes even more burdensome. Thus, the VPN manager becomes a single point of failure for the entire VPN; overload of the VPN manager can cause the entire VPN to fail. This makes the VPN architecture very difficult and very costly to scale, which is not ideal for enterprises relying on secure and private electronic communications.

The Applicants' invention enhances the scalability of a VPN by dividing the member nodes of the VPN, which communicate with each other via encrypted communications, into subsets and providing a plurality of master nodes that are each associated with a subset of member nodes to control membership (*i.e.*, admission and departure) in the VPN and to facilitate VPN communications for that subset. For example, each master node is responsible for managing the generation and distribution of encryption keys for only its associated subset(s), so that VPN communication and

PAGE 19/22 * RCVD AT 2/16/2006 6:10:36 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/32 * DNIS:2738300 * CSID:732 530 9808 * DURATION (mm-ss):07-42

management burdens are not placed entirely on a single master node. This eliminates the single point of failure, because if one master node fails, any one of a plurality of other master nodes is available to assume the failed node's responsibilities. Thus, a VPN employing such an architecture is more easily scalable than a VPN employing a more conventional architecture, because a plurality of new member nodes may be added or admitted to the VPN through a discrete master node.

The Applicants' invention positively claims the communication facilitation function of the master node. That is, in at least claims 1, 18 and 35, the Applicants recite the limitation of a master node that facilitates VPN communications between members of a VPN. As described above, Bots does not teach or suggest a mechanism for facilitating VPN communications between member nodes of a VPN, but rather teaches a communication intercept point. Bots thus fails to teach or anticipate a virtual private network (VPN) in which master nodes control admission and departure in the VPN for an associated non-empty subset of member nodes, as well as facilitate VPN communications between the member nodes, as positively claimed by the Applicants in claims 1, 18 and 35. Therefore, for at least the reasons set forth above, the Applicants submit that independent claims 1, 18 and 35, as amended, fully satisfy the requirements of 35 U.S.C. §102 and are patentable thereunder.

Dependent claims 2-3, 19-20 and 36-37 depend from claims 1, 18 and 35 and recite additional features therefore. As such, and for at least the reasons set forth above, the Applicants submit that claims 2-3, 19-20 and 36-37 are not anticipated by the teachings of Bots. Therefore, the Applicants submit that dependent claims 2-3, 19-20 and 36-37 also fully satisfy the requirements of 35 U.S.C. §102 and are patentable thereunder.

II. REJECTION OF CLAIMS 4-17, 21-34 and 38-51 UNDER 35 U.S.C. § 103

Claims 4-17, 21-34 and 38-51 stand rejected as being unpatentable over Bots in view of the Pandya et al. patent (United States Patent No. 6,671,724, issued December 30, 2003, hereinafter "Pandya"). In response, the Applicants have cancelled claims 7, 24 and 41 without prejudice and have amended independent claims 1, 18 and 35, from

PAGE 20/22 * RCVD AT 2/16/2006 6:10:36 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/32 * DNIS:2738300 * CSID:732 530 9808 * DURATION (mm-ss):07-42

which claims 4-6, 8-17, 21-23, 25-34, 38-40 and 42-51depend, in order to more clearly recite aspects of the present invention.

Particularly, the Examiner's attention is directed to the fact that Pandya, like Bots, fails to disclose or suggest the novel invention of a virtual private network (VPN) in which master nodes control admission and departure in the VPN for an associated non-empty subset of member nodes, as well as facilitate VPN communications between the member nodes, as claimed in Applicants' amended independent claims 1, 18 and 35. Thus, Pandya fails to bridge the substantial gap in the teachings of Bots. Bots in view of Pandya therefore fails to teach or make obvious the invention recited by the Applicants in claims 1, 18 and 35. Therefore, for at least the reasons set forth above, the Applicants submit that independent claims 1, 18 and 35, as amended, fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

Dependent claims 4-6, 8-17, 21-23, 25-34, 38-40 and 42-51 depend from claims 1, 18 and 35 and recite additional features therefore. As such, and for at least the reasons set forth above, the Applicants submit that claims 4-6, 8-17, 21-23, 25-34, 38-40 and 42-51 are not made obvious by the teachings of Bots in view of Pandya. Therefore, the Applicants submit that dependent claims 4-6, 8-17, 21-23, 25-34, 38-40 and 42-51 also fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

III. CONCLUSION

Thus, the Applicants submit that all of the presented claims fully satisfy the requirements of 35 U.S.C. §102 and 35 U.S.C. §103. Consequently, the Applicants believe that all of the presented claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the issuance of a final action in any of the claims now pending in the application, it is requested that the Examiner telephone Mr. Kin-Wah Tong, Esq. at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously

PAGE 21/22 * RCVD AT 2/16/2006 6:10:36 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/32 * DNIS:2738300 * CSID:732 530 9808 * DURATION (mm-ss):07-42

as possible.

Respectfully submitted,

2/16/06
Date

Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 530-9404

Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702

PAGE 22/22 * RCVD AT 2/16/2006 6:10:36 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/32 * DNIS:2738300 * CSID:732 530 9808 * DURATION (mm-ss):07-42